Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada

Canada

Treasury Board Identity Management Policy and Pan-Canadian Trust Framework

Identity Management Policy Workshop

Workshop Objectives

Policy Overview & Federated Identity

- Overview of TB Policy Suite Architecture
- PGS – Identity Management
- Identity as a starting point for Services & Benefits
- Drive to Digital Identity
- Federated Approach

Pan-Canadian Identity Validation Standard

Guideline on Defining Authentication Requirements

Guideline on Identity Assurance

CSE User Authentication Guidance for IT Systems

Case Studies

Annexes – Additional information

Policy Overview
&
Federated Identity

Policy Foundation and Application

Issued under Policy on Government Security (PGS)

2009: Directive on Identity Management ***(applies to employees, external clients, organizations, and devices)***

2011: Federating Identity Management in the GC

2012: Guideline on Defining Authentication Requirements

2013: Standard on Identity and Credential Assurance

2015: Guideline on Identity Assurance

2016: CSE User Authentication Guidance for IT Systems

Application	Individuals	Organizations	Devices
Internal *ICAS - Internal Centralized Authentication Service	• GC Employees • Contractors	• Departments / Agencies • Crown Corporations	• Mobile devices
External Access to online services offered to the public	• Citizens • Clients of GC services	• Corporations • Associations • Proprietorships	• Smart devices • IoT

Security Policy Architecture

NEW (PROPOSED)

Legislation

Financial Administration Act

Policies

Policy on Government Security

Directives

Directive on Security Management

Mandatory Procedures on Security Controls

- Security Screening
- Security Awareness & Training
- Business Continuity Management
- Information Management Security
- Information Technology Security
- Physical Security
- Security in Contracts and Other Arrangements
- Security Event Management

Directive on Identity Management

Mandatory Procedures and Standards

Standard on Security Categorization

Standard on Acceptable Network and Device Use

Standard on Security Event Reporting

Standard on Identity and Credential Assurance

NOTE: *Standard on Security Screening* not included in the reset exercise

Guidelines and Tools

Detailed Government-wide Responsibilities

Guideline on Developing a Departmental Security Plan

Other Guidelines and Tools

GC Security Event Management Protocols

Guideline on Identity Assurance (2015)

Lead Security Agencies Guidance and Tools

CURRENT (OLD)

Legislation

Financial Administration Act (FAA)

Policies

Policy on Government Security (PGS) (2009 – amended 2012)

Policy on Acceptable Network and Device Use (PANDU) (2013)

Directives

Directive on Departmental Security Management (DDSM) (2009)

Directive on Identity Management (2009)

Mandatory Procedures and Standards

Security Organization & Administration (1994)

Readiness Levels for Federal Government Facilities (2002)

Identity and Credential Assurance (2013)

Security Screening (2014)

Management of Information Technology Security (2004)

Business Continuity Planning (2004)

Physical Security (2004)

Security in Contracting (1994)

Guidelines and Tools

Developing a Departmental Security Plan

Security Screening and Security in Contracting Guidelines and Tools (e.g. briefing form, SRCL)

Guideline on Identity Assurance (2015)

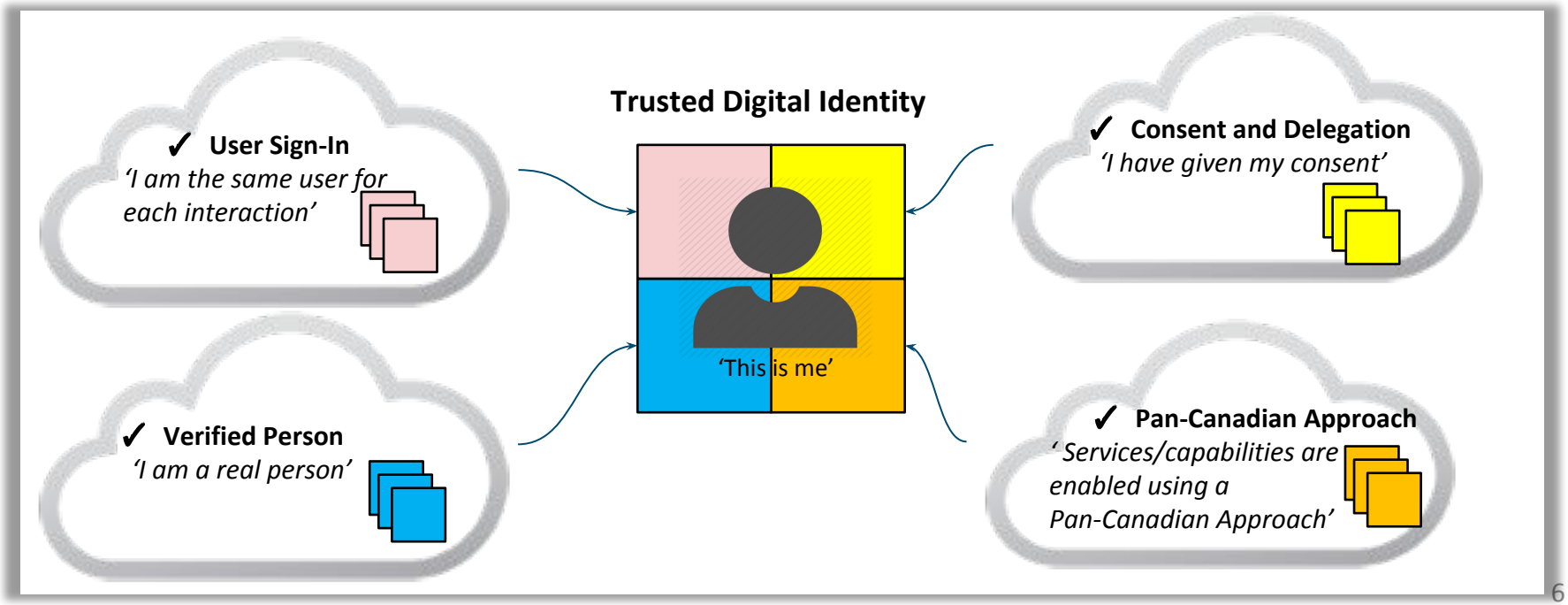
Information Technology Incident Management Plan

Lead Security Agencies Guidance and Tools

Trusted Digital Identity

New PGS Definitions:

- **trusted digital identity**: An electronic representation of a person, used exclusively by that same person, to receive valued services and to carry out transactions with trust and confidence.
- **trust framework:** A set of agreed on definitions, principles, conformance criteria, assessment approach, standards and specifications.



Directive on Identity Management

New requirements:

4.1.7. Accepting **trusted digital identities** provided through an approved **trust framework** as an equivalent alternative to in-person interactions, through an assessment of the following processes:

- ✓ **Identity and program-specific information**
- ✓ **Identity and credential assurance** (according to Standard on Identity and Credential Assurance)
- ✓ **Identity enrolment**
- ✓ **Notification and consent**

4.1.9 Using mandatory enterprise services for identity management, credential management and cyber authentication.

Identity and Authentication in Service Context

To fulfil client service, personal information collected to

1) Establish person is who they claim to be (identity proofing)
   - In future, could include validation of personal information with Provinces/Territories
2) determine benefit entitlement/eligibility

Desired outcome: provide high quality (digital) services and improved client experience through

- seamless online transactions with GC institutions through single, secure login
- re-use of personal information for various government services without need to re-enter with each application for service (tell-us-once)
- Minimizing cyber security risk through single secure log in

Identity: Starting Point for Services & Benefits

Today, identity is managed separately by each sector…

Financial Sector

Who are you?

How will you pay?

Identity risks
translate into:

Sector Issues
- Financial fraud
- Money laundering
- Higher transaction fees

Public Sector

Who are you?

Are you eligible for a government benefit?

Identity risks
translate into:

Sector Issues
- Benefits fraud
- Longer processing times
- Redundant processes

Healthcare Sector

Who are you?

What is your medical history?

Identity risks
translate into:

Sector Issues
- Prescription fraud
- Patient Privacy
- Record integrity

… but the impacts are felt by everyone

The Drive to Digital Service Delivery

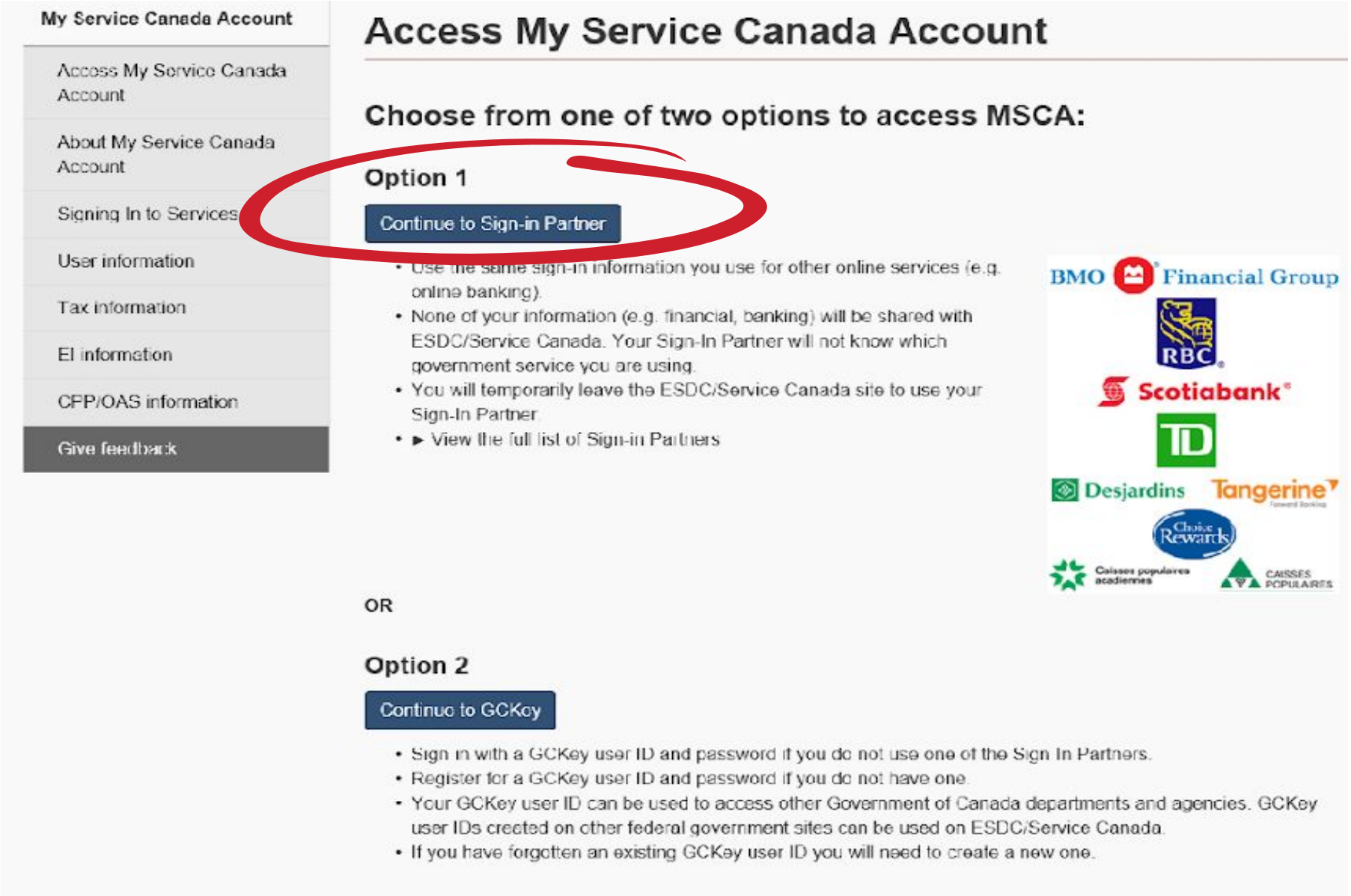
Priorities

- Creation of a Single Online Window
- Citizen-focused digital service delivery
  - Access to information
  - Improved client experience
  - Web Renewal: Canada.ca portal

Strategy

- Policy to enable standardized services
- Leverage private sector solutions
- Enable federated identity across domestic and international boundaries

Choose Sign-In Partner or GCKey



Evolution to Federating Identity

Federating Credentials

Cyber Authentication Service

Mandatory Services

- Commercial
- Government of Canada Issued
- Other jurisdictions

- Standards-based
- Federation

❑ Multiple Recognized Providers
❑ Multiple Credential Options
❑ Multiple Levels of Assurance

Federating Identity

Government of Canada Approach

Government of Canada Identity Federation Service

Pilot Projects

- Government of Canada Identity Assurance Service
  - Government of Canada Identity Validation Service

- Policy Enablers
- Standards-based
- Federation

❑ Government of Canada Identity Validation Service
❑ Identity Business & Technical Architecture

Pan-Canadian Approach

Identity Federation Service

Federation Enablers

- Identity Services
  - Identity Federation Services
  - Credential Federation Services

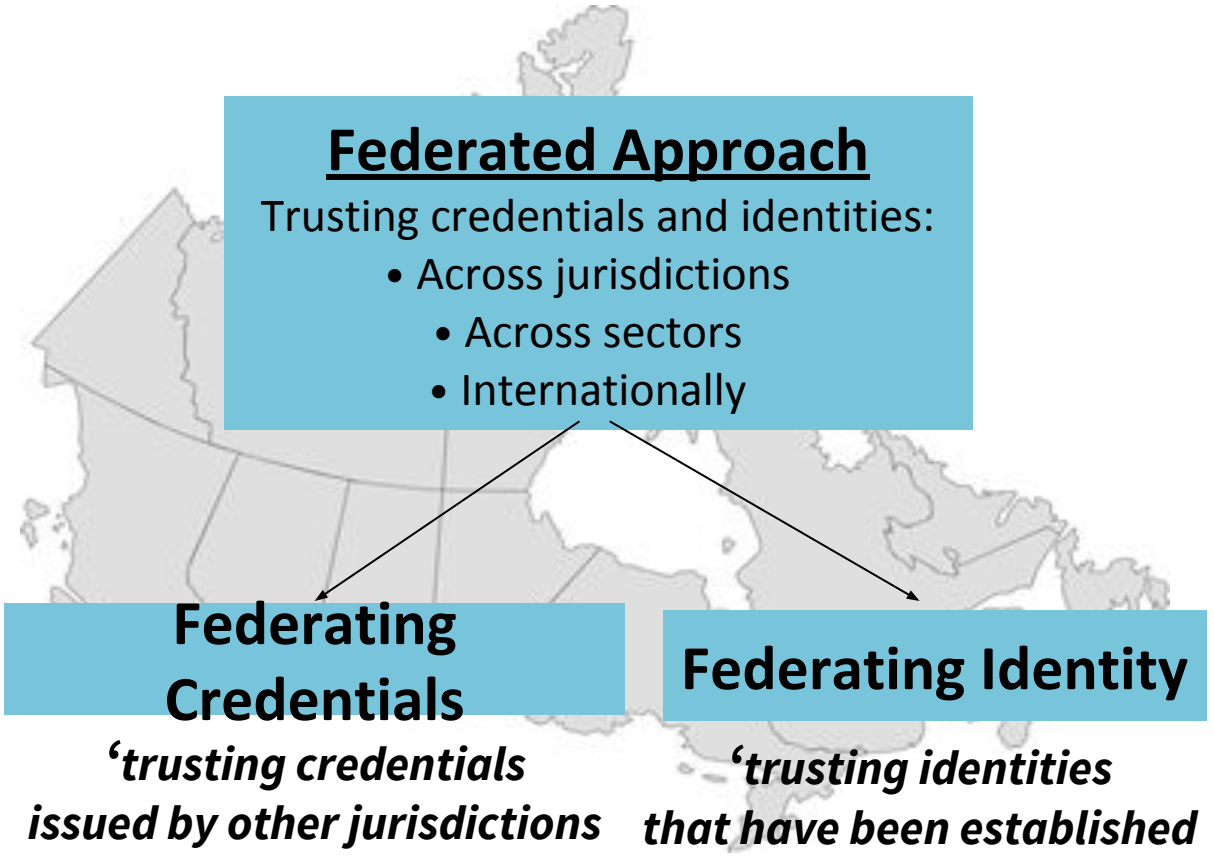
- Legislative Enablers
- Standards-based
- Federation

❑ Commercial Services
❑ Multiple Authoritative Identity Sources

Pan-Canadian Collaboration

Principles:

- ✓ Respects privacy
- ✓ Client choice
- ✓ Governments play key role
- ✓ Collaborate with trusted Federal, Provincial, Territorial and private sector institutions
- ✓ Phased approach to evolving services and infrastructure



Pan-Canadian Policy Direction

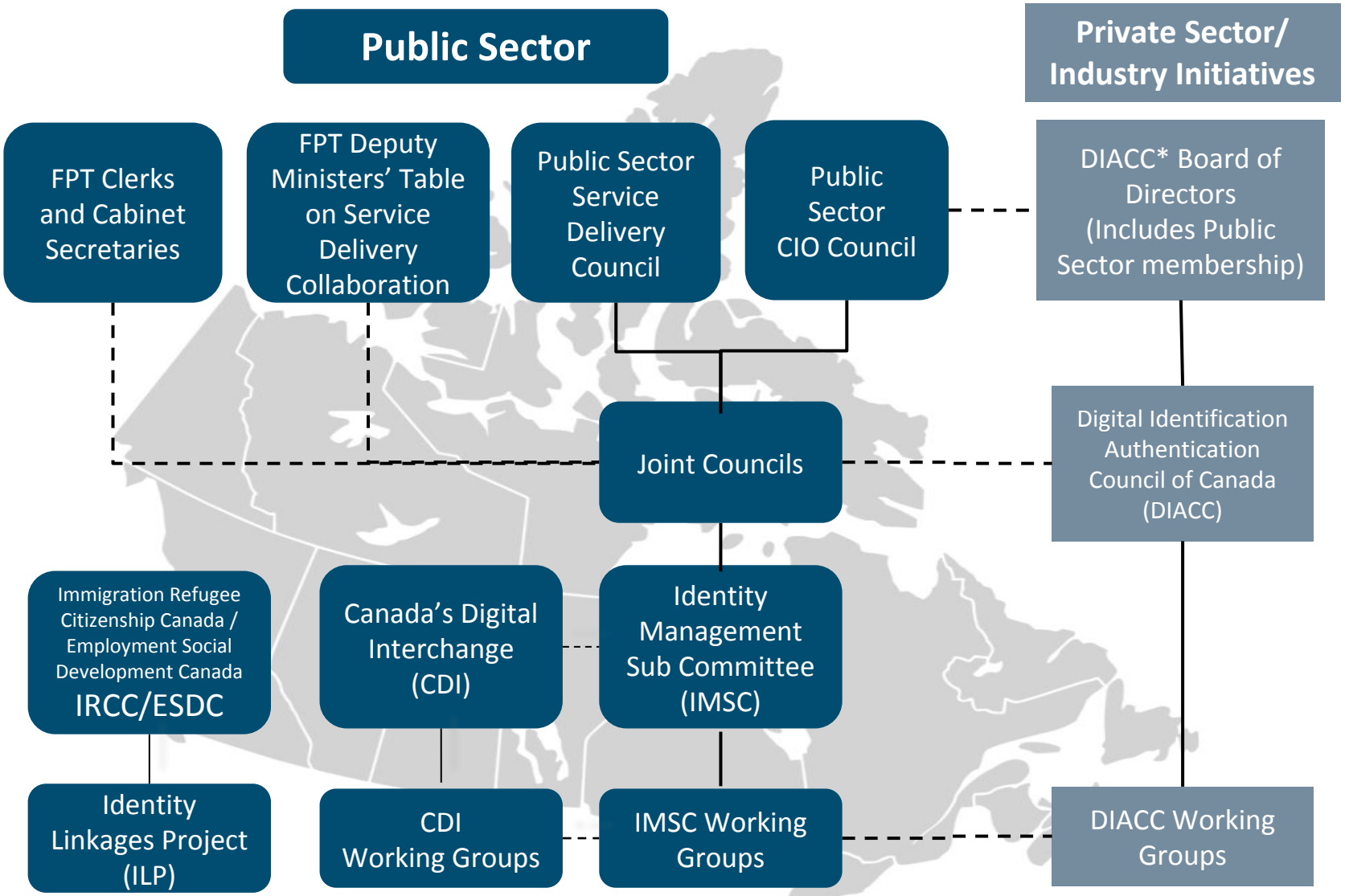
2014: Identity Validation Standard

2016/17: Pan-Canadian Trust Framework

(Technical Standards, Specifications, Certifications, Privacy, Security, Service delivery, Organizational)

Pan-Canadian Trust Framework

Pan-Canadian Trust Framework: Context



Other Initiatives Underway

- Death Notification Project
- Business Number or Expedited Business Start
- DIACC Proof of Concept for Residency

**Digital Identification and Authentication Council of Canada*

Building a Pan-Canadian Trust Framework

Trusted Digital Identity

Including Public Sector and Private Sector Considerations

Is it the same person?

Verified Login

- ❑ Credential Issuance
- ❑ Credential Authentication
- ❑ Credential Recovery
- ❑ Credential Revocation

Is it a real/existing person?

Verified Person

- ❑ Identity Resolution
- ❑ Identity Establishment
- ❑ Identity Validation
- ❑ Identity Verification
- ❑ Identity Maintenance

Has the user given consent?

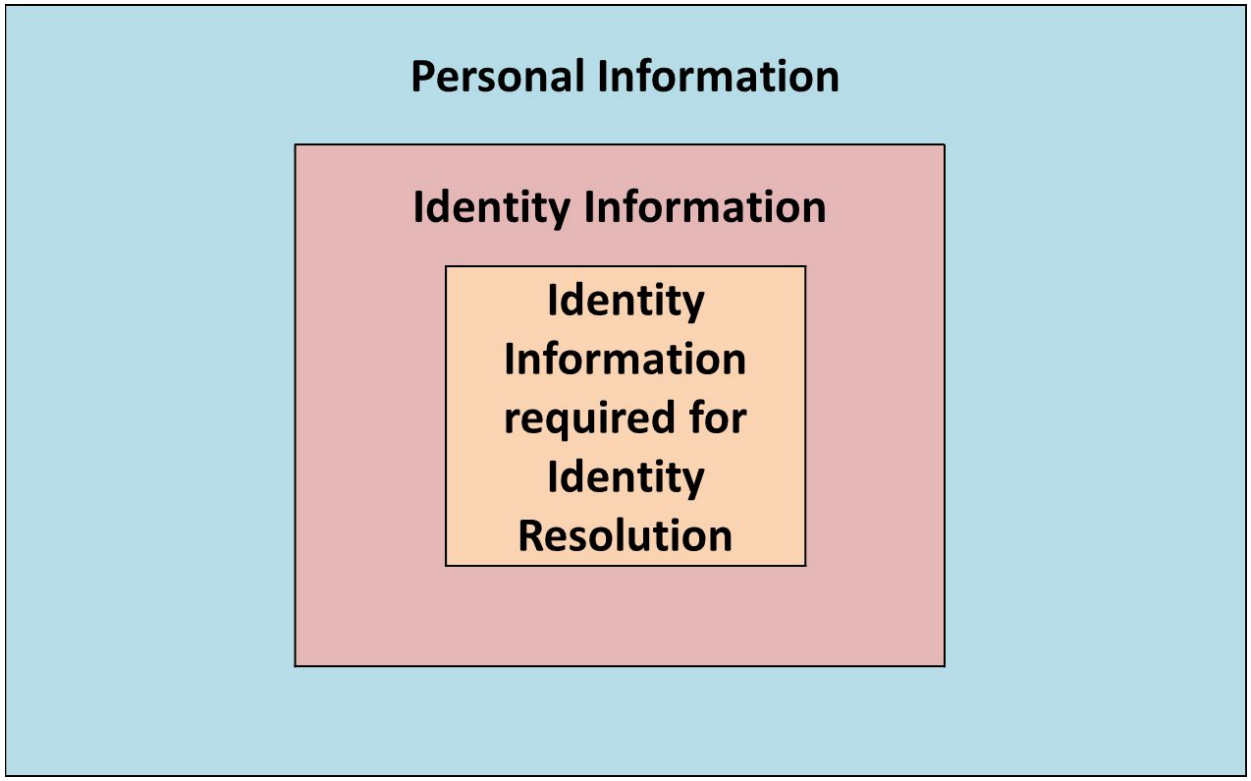
Consent and Delegation

- ❑ Credential Determination
- ❑ Identity Linking
- ❑ Owner Authorization

Pan-Canadian Infrastructure

Technical Standards, Specifications, Certifications Privacy, Security, Service Delivery, Organizational

Pan-Canadian Standardized Concepts



The Personal Information Categories

1. PERSON NAME
2. DATE OF EVENT
3. PLACE OF EVENT
4. SEX, GENDER, DOCUMENTED SEX
5. ASSIGNED IDENTIFIER
6. PERSON STATUS
7. ADDRESS
8. ASSOCIATED PERSON
9. BIOMETRIC IMAGE
10. PERSON AGE
11. CONTACT DETAIL
12. BIRTH VITAL EVENT DETAIL
13. DEATH VITAL EVENT DETAIL
14. STILLBIRTH VITAL EVENT DETAIL

Personal Information Categories by Function

Personal Information Category	Function		
PERSON NAME	Validation	Retrieval	Notification
DATE OF EVENT			
PLACE OF EVENT			
SEX, GENDER, DOCUMENTED SEX			
ASSIGNED IDENTIFIER			
PERSON STATUS			
ADDRESS			
ASSOCIATED PERSON			
BIOMETRIC IMAGE			
PERSON AGE			
CONTACT DETAIL			
BIRTH VITAL EVENT DETAIL			
DEATH VITAL EVENT DETAIL			
STILLBIRTH VITAL EVENT DETAIL			

Guideline on Defining Authentication Requirements

Evolution of Authentication

'State of the art' authentication practices are rapidly evolving

- More holistic, adaptive and responsive approach to authentication
- Credential authentication is now considered part of an overall 'layered security' scheme that can be employed to mitigate risk. Examples include
  - Device identification, challenge questions, Out-of-band transmission, Suspicious activity detection and response
- 'weakness in one control may be compensated for by the strength of a different control' (Revised Federal Financial Institution Examination Council Guidance 2011 - USA)

Recently published guidance documents are defining 'compensating factors' (or 'compensating controls') as a key concept to address the following:

- Added flexibility to authenticate users in many contexts and scenarios (e.g. domestic vs. international, browser vs. mobile apps, account-to-account access)

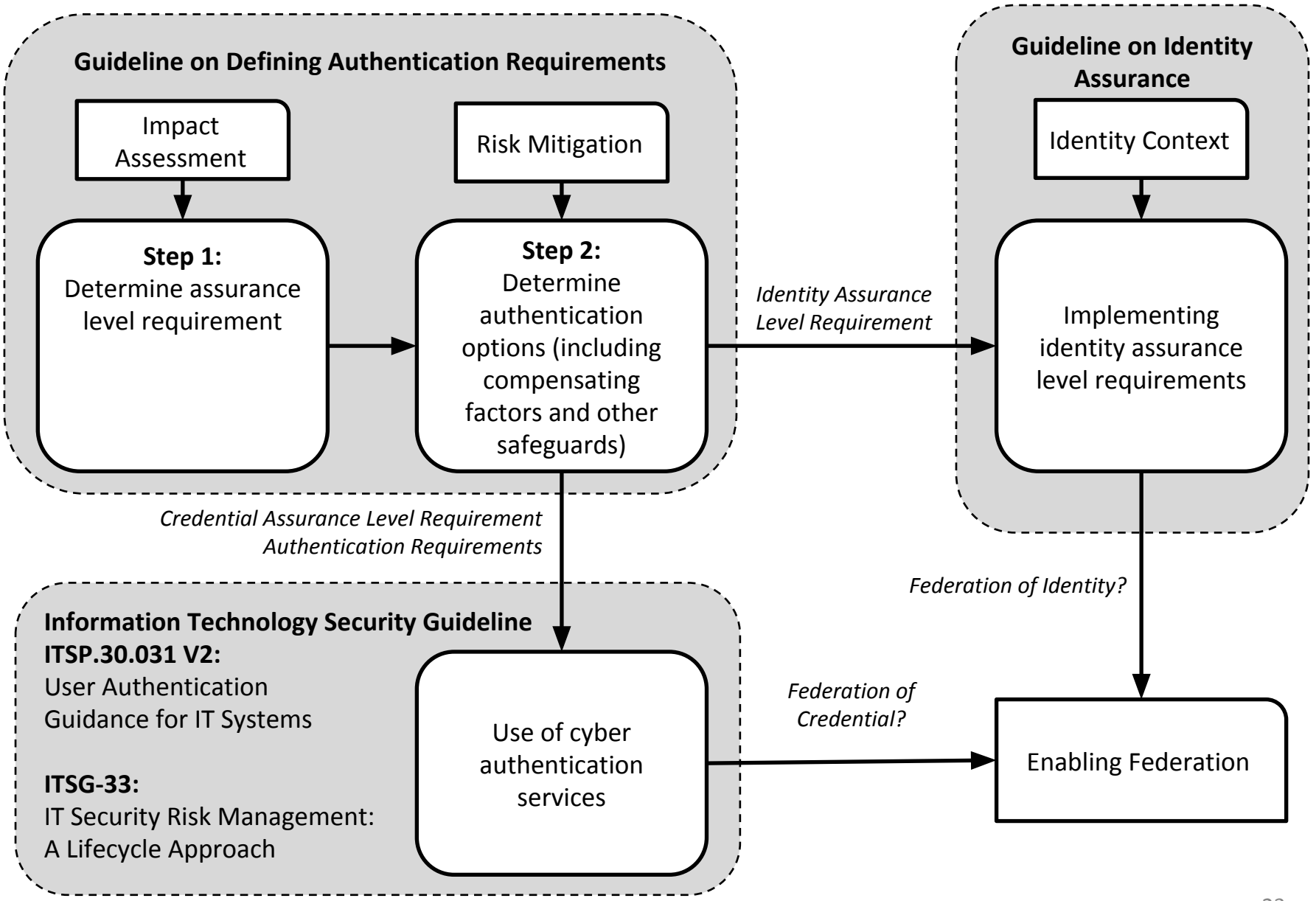
Guideline on Defining Authentication Requirements

Purpose of Guidance:

- Sets out Government of Canada direction
- Assists departments and agencies to define their authentication requirements relative to program and service delivery requirements
- Enables departments to use standardized approaches while retaining flexibility to further define requirements as necessary

Tools Provided:

- Assurance Level Requirement Worksheet
  - Comprehensive assessment approach to determine a standardized level of assurance requirement
- Determination of Authentication Requirements
  - Identity Assurance Requirements
  - Credential Assurance Requirements
  - Authentication Solution Requirements
  - Compensating Factors, Other Safeguards and Acceptable Risk


Guideline on Defining Authentication Requirements
Impact Assessment
Risk Mitigation
Step 1:
Determine assurance level requirement
Step 2:
Determine authentication options (including compensating factors and other safeguards)
Identity Assurance Level Requirement
Guideline on Identity Assurance
Identity Context
Implementing identity assurance level requirements
Credential Assurance Level Requirement
Authentication Requirements
Federation of Identity?
Information Technology Security Guideline
ITSP.30.031 V2:
User Authentication Guidance for IT Systems
ITSG-33:
IT Security Risk Management: A Lifecycle Approach
Use of cyber authentication services
Federation of Credential?
Enabling Federation

Approach to Defining Requirements

Collaboration between Program/Service owners & IT/Security practitioners…

Performed by the program/service owners

Impact Assessment determines the level of assurance required

Answers the question

What level of assurance do I need to achieve my program objectives?

Assurance Level Requirement

Level 4
Very high confidence required

Level 3
High confidence required

Level 2
Some confidence required

Level 1
Low confidence required

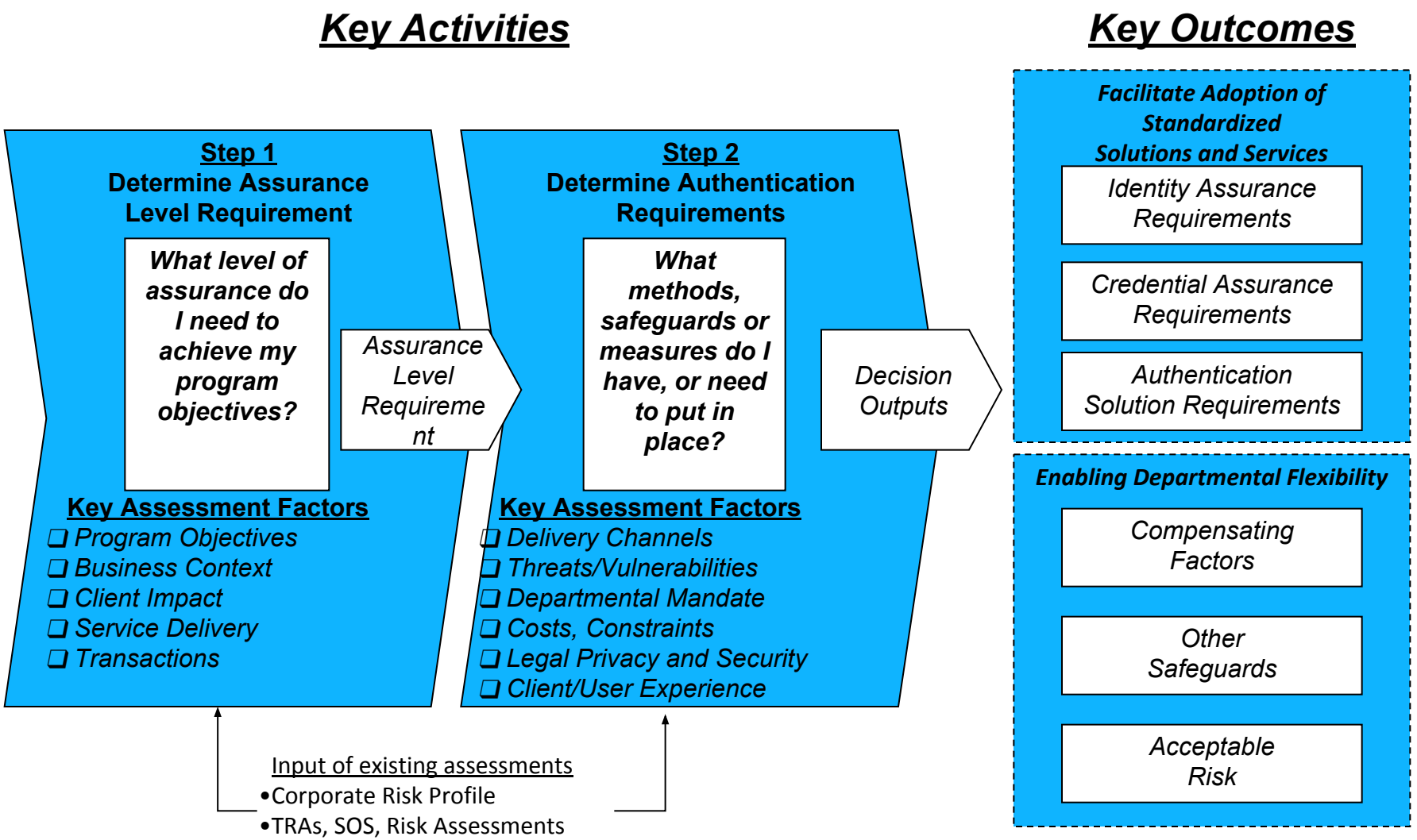
Performed by security and IT practitioners

Selection of Controls uses standardized requirements (where possible), compensating factors, and acceptable risk

Answers the question

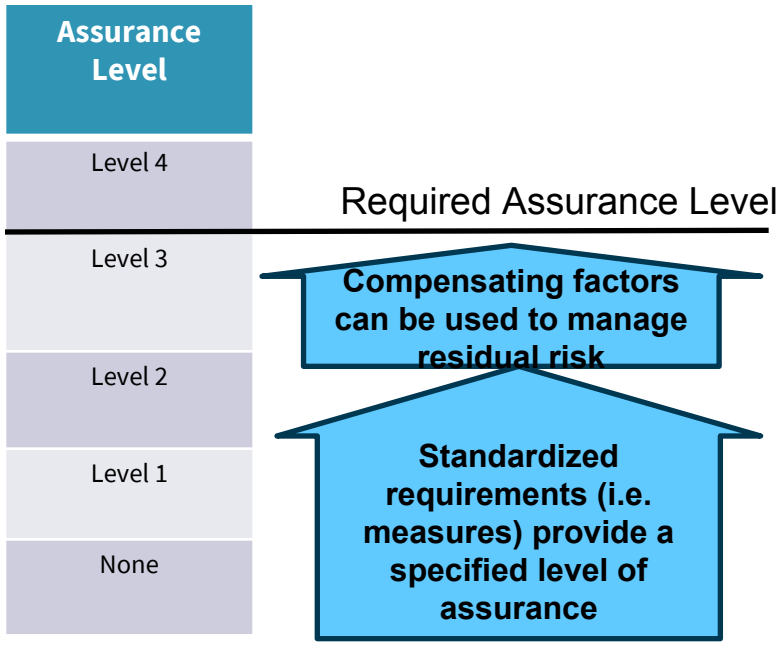
What methods, safeguards or measures do I have, or need to put in place?

Major Steps in Defining Requirements



Compensating Factors

- Additional measure employed during the authentication process that reduces the likelihood of an authentication error (also referred to as compensating control)
- Compensating factors may be employed when a specific control does not provide a required assurance level (due to cost, usability, etc.)
- Examples
  - Shared secrets
  - Validation of identity information, program information
  - Token/grid card challenge, IP address, device confirmation
  - Out-of-band (e.g. call to mobile)



Use of Compensating Factors, Other Safeguards and Acceptable Risk

Defined in guidance

- **Compensating Factors** – additional safeguards employed during the authentication process
- **Other Safeguards** – use of other security control mechanisms that are outside of the authentication process (e.g. downstream security controls) which can also mitigate risk
- **Residual Risk** –Residual risk can be mitigated using compensating controls and/or other safeguards

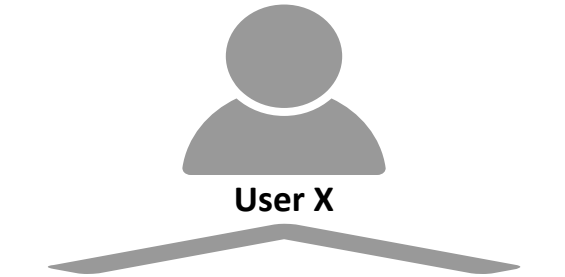
These concepts enable departments to have flexibility in determining their optimal authentication solution requirements. Departments must decide on:

- Adoption of commercial services and use of standardized requirements
- Use of compensating controls, and/or safeguards to mitigate residual risk.

Guideline on Identity Assurance

Credential and Identity Assurance

Credential Assurance

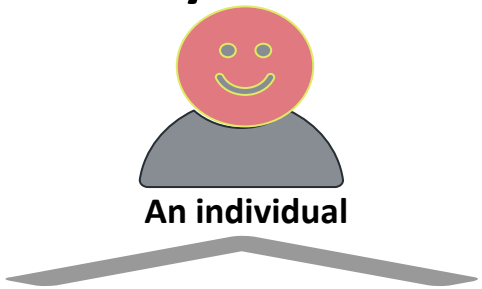


Binding a credential to a unique individual

Assurance Levels

Level 4	Very high confidence required
Compromise: serious to catastrophic harm	
Level 3	High confidence required
Compromise: moderate to serious harm	
Level 2	Some confidence required
Compromise: minimal to moderate harm	
Level 1	Little confidence required
Compromise: nil to minimal harm	

Identity Assurance



Establishing the real identity of an individual

Assurance Levels

Level 4	Very high confidence required
Compromise: serious to catastrophic harm	
Level 3	High confidence required
Compromise: moderate to serious harm	
Level 2	Some confidence required
Compromise: minimal to moderate harm	
Level 1	Little confidence required
Compromise: nil to minimal harm	

Overview of Guideline on Identity Assurance

Provides implementation guidance on four requirements specified in Appendix C of the Standard on Identity and Credential Assurance:

1. **Uniqueness:** An identity must be unique
   - Definition of identity information (versus program information)

2. **Evidence of Identity:** Evidence must support the claims made by an individual
   - Foundational and supporting evidence of identity

3. **Accuracy of Identity Information:** Identity information must be accurate
   - Confirmation of identity information using an authoritative source

4. **Linkage of identity information to individual:** Identity information must relate to the individual making the claim.
   - Linkage methods: knowledge-based, biological/behavioural characteristics, trusted referee, physical possession

Overview of Guideline (cont'd)

Provides guidance on integrating identity assurance into departmental business and system processes:

- Efficient and Transparent Procedures
- Privacy Concerns
- Linkage and Binding
- Using Identity Lifecycle Models

Federation consideration for departments when:

- Acting in the role of an authoritative or relying party
- A member or not a member of a federation

Considerations for main types of fraud:

- Document,
- Record
- Impostor

Example: Establishing Identity Assurance (for Level 3)

Requirement	Level 3 Identity Assurance
Uniqueness	Define identity information Define context
Evidence of Identity	**Two** instances of evidence of identity
Accuracy of Identity Information	Identity information acceptably matches assertion by an individual and all instances of evidence of identity **and** Confirmation of the foundational evidence of identity using authoritative source **and** Confirmation that supporting evidence of identity originates from appropriate authority, using authoritative source **or** inspection by trained examiner
Linkage of Identity Information to Individual	At least **one** of the following: i. Knowledge-based confirmation ii. Biological or behavioural characteristic confirmation iii. Trusted referee confirmation iv. Physical possession confirmation

Standard on Identity and Credential Assurance Appendix C: Minimum Requirements

Requirement	Level 1	Level 2	Level 3	Level 4
Uniqueness	Define identity information Define context			
Evidence of Identity	No restriction on what is provided as evidence	**One** instance of evidence of identity	**Two** instances of evidence of identity (At least one must be foundational evidence of identity.)	**Three** instances of evidence of identity (At least one must be foundational evidence of identity.)
Accuracy of Identity Information	Acceptance of self-assertion of identity information by an individual	Identity information acceptably matches assertion by an individual and evidence of identity **and** Confirmation that evidence of identity originates from appropriate authority	Identity information acceptably matches assertion by an individual and all instances of evidence of identity **and** Confirmation of the foundational evidence of identity using authoritative source **and** Confirmation that supporting evidence of identity originates from appropriate authority, using authoritative source **or** inspection by trained examiner	Identity information acceptably matches assertion by an individual and all instances of evidence of identity **and** Confirmation of the foundational evidence of identity using authoritative source **and** Confirmation that supporting evidence of identity originates from appropriate authority, using authoritative source **or** inspection by trained examiner

Table continued on next slide…

Standard on Identity and Credential Assurance Appendix C: Minimum Requirements

Table continued from previous slide…

Requirement	Level 1	Level 2	Level 3	Level 4
Linkage of Identity Information to Individual	No requirement	No requirement	At least **one** of the following: i) Knowledge-based confirmation ii) Biological or behavioural characteristic confirmation iii) Trusted referee confirmation iv) Physical possession confirmation	At least **three** of the following: i) Knowledge-based confirmation ii) Biological or behavioural characteristic confirmation iii) Trusted referee confirmation iv) Physical possession confirmation

Note: When the authoritative source is outside of Canadian jurisdiction, the accuracy of identity information will be determined through a risk-managed approach.

Assurance Level Impact Assessment Summary Table

Name of Program/Service/Transaction:				
Assessment Question:	***If this program, service or transaction benefits the wrong person, would it like result in… (complete each question using the table cells below)***			
Assessment Category	**Level 1 Assessment**	**Level 2 Assessment**	**Level 3 Assessment**	**Level 4 Assessment**
1. Inconvenience, distress/loss of standing or reputation	❑	❑	❑	❑
2. Financial loss	❑	❑	❑	❑
3. Harm to program or public interest	❑	❑	❑	❑
4. Unauthorized release of sensitive personal or commercial information.	❑	❑	❑	❑
5. Unauthorized release of sensitive government information.	❑	❑	❑	❑
6. Civil or criminal violations	❑	❑	❑	❑
7. Personal Safety	❑	❑	❑	❑
8. National security	❑	❑	❑	❑
ASSURANCE LEVEL REQUIREMENT	❑ **Minimum Level 1 Required**	❑ **Minimum Level 2 Required**	❑ **Minimum Level 3 Required**	❑ **Minimum Level 4 Required**

Example: Passport Program

Eight service lines were assessed (two detailed assessments are below)

Summary of Assurance Level Requirements

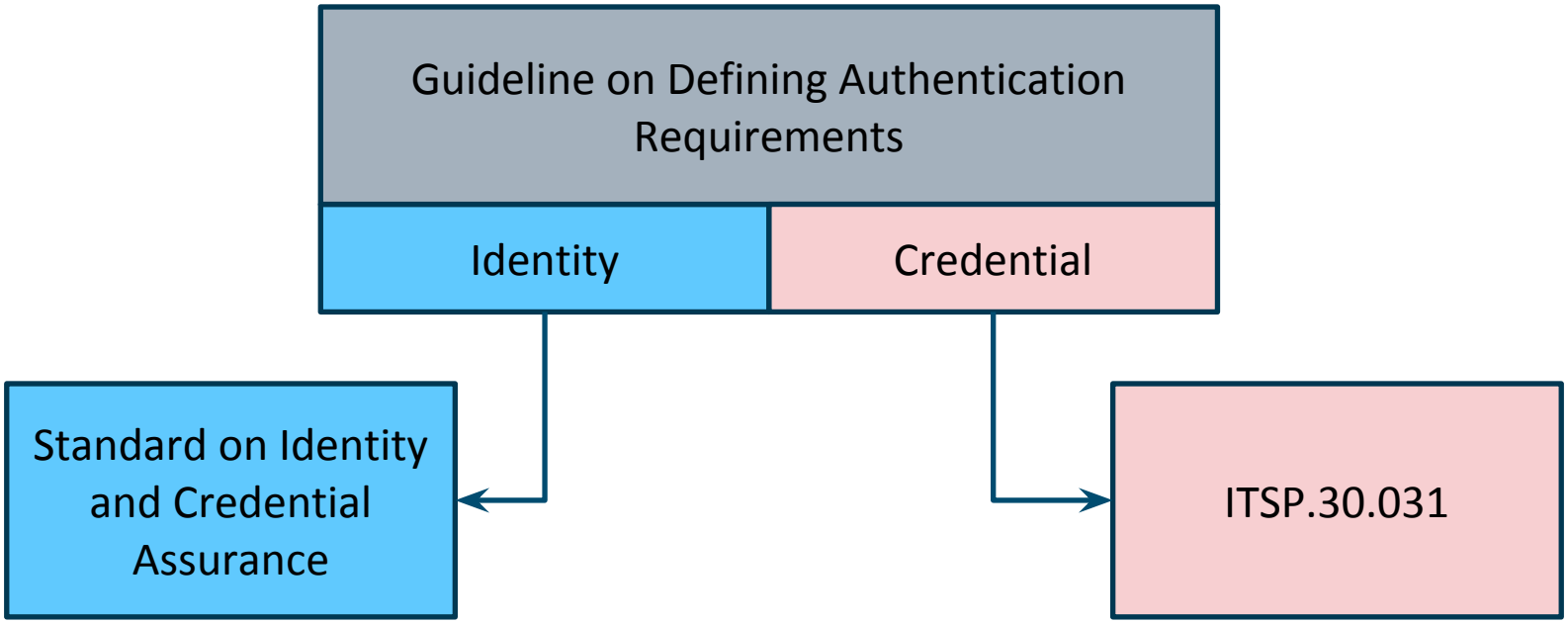
Passport Canada Product	Assurance Level Requirement
Adult Regular Passport	[redacted]
Children's Passport	
Emergency Travel Document	
Temporary Passport	
Diplomatic Passport	
Special Passport	
Refugee Travel Document	
Certificate of Identity	

Any travel document issued in the name of a minor has an Assurance Level Requirement of 4, even if the adult version of the travel document was assessed at a lower level.

CSE User Authentication Guidance for IT Systems

Relation to TBS Guidelines

- **The TBS *Guideline on Defining Authentication Requirements* separates authentication into identity assurance and credential assurance.**
- **ITSP.30.31 provides the guidance for credential assurance.**



Levels of Assurance - Recommended use in the GC

- **Examples of recommended uses of LoA credentials in the GC:**

LoA	Recommended Use in the GC
1	Not recommended for GC use.
2	End-user access to systems or information.
3	Administrative access to systems or information.
4	Administrative access to high-value systems or information.

Levels of Assurance Applied to Tokens

- **ITSP.30.031 provides a framework for selecting authentication solutions:**

LoA	Main Characteristic	Examples
1	Basic authentication methods – not recommended for GC use.	Password or PIN systems with poorly secured databases and/or recovery methods
2	Standard, typically single-factor end-user authentication solutions	Memorized Secret Tokens, Pre-Registered Knowledge Tokens, Look-up Secret Tokens, Out of Band Tokens, software cryptographic tokens, and Single Factor One-Time Password Devices
3	Two-factor authentication methods using a hardware factor	Passwords/PINS combined with OTP Tokens and Smartphones
4	Two-factor authentication with a cryptographically-based hardware factor	Hardware cryptographic tokens, multi-factor One-Time-Password devices

Case Studies

Case Study: Passport Program

Context

- Small organization
- Comparably few products/programs to assess
  - Eight travel document products
- Highly visible and used product

Preparation

- Briefings at senior management committees on Standard and Guideline during drafting stages
- Preparatory briefing on assessments with affected senior managers

Key Lessons

- Importance of organizational awareness of impacts
- Conduct assessments as soon as possible

Case Study: Passport Program

Conducting the Assessments

- Gathered key players
  - Senior managers from Operations (Chief Operating Officer), Security, and Policy
  - Invited subject matter experts from Treasury Board to observe and advise
- Opened session with review of key sections of Guidelines to ensure common understanding of task and methodology
- Reviewed all eight products in one session
  - Allowed for consistency of application of Guideline
- Used a custom grid to methodically assess each product across all eight categories of harm
  - Obtained consensus on each category before advancing to the next
  - Documented the rationale for each decision

Key Lessons

- In addition to program experts, include SME on the TB policy suite
- Provide custom tools
- Debates can digress, ensure a strong chair manages the discussion

Case Study: Passport Program

Documenting the Results

- Prepared a separate assessment for each product
- Documented the rationale for *each* category of harm
- Consulted with legal services
- Documented any change to agreed upon levels under separate cover
- Circulated for approval by participating senior managers and legal services

Key Lessons

- When in doubt – Consult
- Some levels will likely change as rationale is elaborated
- If possible, have dedicated resource(s) for project to see it through from beginning to end

Case Study: CRA

Overview

- The CRA offers numerous online services for individuals, businesses and representatives
- The CRA establishes an identity assurance, through processes and IT systems, when there is a need to know who is at the other end of the computer
- An Identity Assurance Risk Assessment is completed for each new or modified service to determine the identity assurance level required

Key Lesson

- Informing impacted stakeholders of the purpose of the risk assessment process allows for a better understanding and appreciation

Case Study: CRA

Risk Assessment Process

- The CRA's risk assessment process involves completing an Assurance Level Requirement Worksheet to:
  - identify categories of harm and impacts to an individual or the Agency
  - evaluate the risks and threats with the proposed or modified online service
- Based on the assessment results, a recommendation with a rationale is prepared and provided to the responsible program area

Key Lesson

- Performing a thorough analysis of the program/service to be implemented is a crucial step in determining the appropriate level of identity assurance

Case Study: CRA

Outcome and Next Steps

- The program area makes the final decision on the service's risk profile as the risk accountability ultimately is borne by functional owners
- Next steps include assisting program area in the determination of the authentication options in order to meet the assurance level requirement

Key Lesson

- Conducting risk assessments at the onset of a project to determine the level of identity assurance saves time and effort

Annex
For Further Information

Annex A - Links to Key Documents

TB/TBS CIO/CSE Approved Versions:

- **Directive on Identity Management:** http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16577
- **Standard on Identity and Credential Assurance:** http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26776
- **Guideline on Defining Authentication Requirements:** http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26262
- **Guideline on Identity Assurance:** http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=30678
- **User Authentication Guidance for IT Systems:** https://www.cse-cst.gc.ca/en/node/1842/html/26717

Draft Versions

- **Policy on Government Security**: http://www.gcpedia.gc.ca/wiki/Policy_Suite_Reset/Security

Annex B - Key PGS Definitions

Term	Definition
Credential	A unique physical object or electronic identifier issued to, or associated with, an individual, organization or device.
Evidence of Identity	A record from an authoritative source indicating an individual's identity. There are two categories of evidence of identity: foundational and supporting.
Foundational Evidence of Identity	Evidence of identity that establishes core identity information such as given name(s), surname, date of birth and place of birth. Examples include records of birth, immigration or citizenship from an authority with the necessary jurisdiction.
Identity	A reference or designation used to distinguish a unique individual, organization or device.
Supporting Evidence of Identity	Evidence of identity that corroborates the foundational evidence of identity and assists in linking the identity information to an individual. It may also provide additional information such as a photo, signature or address.
Trust Framework	A set of agreed on definitions, principles, conformance criteria, assessment approach, standards, and specifications.
Trusted Digital Identity	An electronic representation of a person, used exclusively by that same person, to receive valued services and to carry out transactions with trust and confidence.

Annex C - Pan-Canadian Definitions

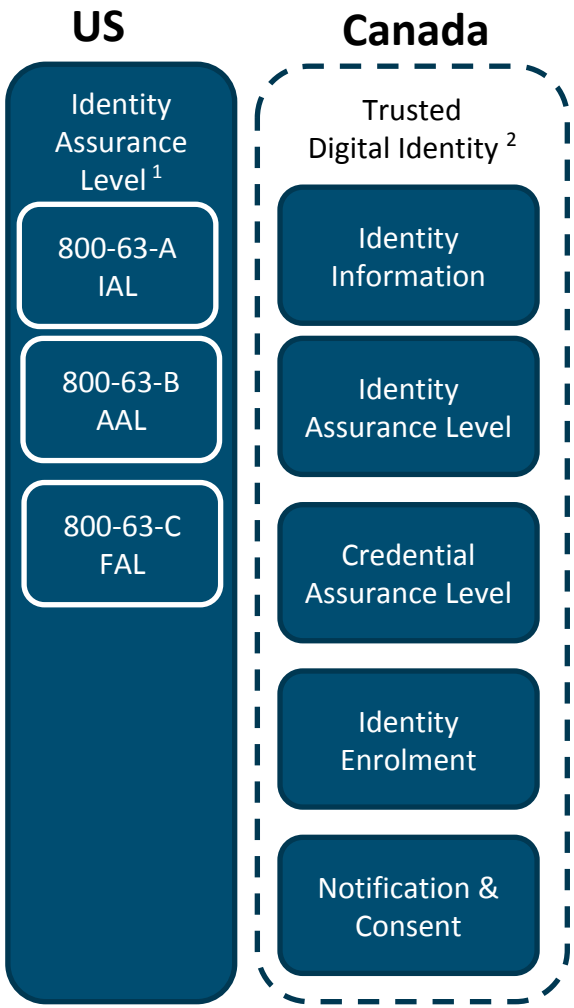
Term	Definition
Identity resolution	The establishment of the uniqueness of a person within a program/service population through the use of identity information
Identity validation	The confirmation of the accuracy of identity information about a person as established by an authoritative party
Identity verification	The confirmation that the identity information being presented relates to the person who is making the claim
Assigned Identifier	An artificial identity attribute that is used solely for the purpose of providing identity uniqueness
….	

Annex D - US-Canada Mapping

Standards and Guidance Mapping

Common Process Patterns	US	Canada
Assessment	✓ OMB M04-04	✓ Directive on Identity Management ✓ Guideline on Defining Authentication Requirements
Unique identification • **Uniqueness**	✓ NIST SP 800 63 A (draft)	✓ Guideline on Identity Assurance
Identity Proofing • **Evidence of identity** • **Identity validation** • **Identity verification**	✓ NIST SP 800 63 A (draft)	✓ Guideline on Identity Assurance
Credential Management • **Lifecycle Management** • **Issuance** • **Authentication**	✓ NIST SP 800 63 B (draft)	✓ User Authentication Guidance for Information Technology Systems ✓ Cyber Authentication Technical Specification 2.1
Enrolment Binding	✓ NIST SP 800 63A (draft)	
Notification and Consent	Requirements woven throughout 800-63-A/B/C	
Trust/ Federation	✓ NIST SP 800 63C	✓ Pan-Canadian Trust Framework ✓ PCIM Validation, Notification & Retrieval Standard Suite ✓ PCIM Information Exchange Specification

Concept Mapping



1. *Defined in US OMB M04-04*
2. *Defined in TB Directive on Identity Management*

Annex E - 2014- 2017 Federating Identity: Milestones and Initiatives

Milestones/Deliverables

- ✓ **2004: Secure Channel, including its epass authentication service, operational**
- ✓ **2007: Identity Management & Authentication (IATF) Task Force Report**
- ✓ **2008: Cyber Auth Report on Future Requirements for the Government of Canada**
- ✓ **2009: TBS Directive on Identity Management**
- ✓ **2009: ITSG-31 Authentication Guidance**
- ✓ **2010: Pan-Canadian Assurance Model**
- ✓ **2010: BC Identity Assurance Standard**
- ✓ **2010: BC Evidence of Identity Standard**
- ✓ **2010: BC Electronic Credential & Authentication Standard**
- ✓ **2010: CIC (Passport Program) Facial Recognition capability operational**
- ✓ **2010: Cyber Auth RFP 1/RFP2/RFP3**
- ✓ **2011: Federating Identity for the Government of Canada: Backgrounder[1]**
- ✓ **2011: IMSC Pan-Canadian Approach to Trusting Identities**
- ✓ **2011: National Routing System (NRS) Data Exchanges Standard**
- ✓ **2012: Cyber Authentication Technical Specification**
- ✓ **2012: Guideline on Defining Authentication Requirements**
- ✓ **2012: Federating Identity Broker Architecture**
- ✓ **2013: GC Federated Credential operational**
- ✓ **2013: Standard on Identity and Credential Assurance**
- ✓ **2013 Cyber Auth Close Out Report**
- ✓ **2013: ePassport operational**
- ✓ **2013: Issuing new BC Services Card commenced**
- ✓ **2013: Service Quebec now responsible for clicSÉQUR**
- ✓ **2013: Ontario approves Electronic Identification, Authentication and Authorization (IAA) policy**
- ✓ **2014: Pan-Canadian Identity Validation Standard**
- ✓ **2015: GC Guideline on Identity Assurance**
- ✓ **2015: BC Identity Information Standard**
- ❑ **2016: Pan-Canadian Identity Trust Framework**

Lessons Learned

Strategic Alignment

Initiatives/Oversight

National Routing System

- 2004-2006: Pilot
- 2006-Present: In Production

Cyber Authentication Renewal

- 2008: Creation of DM Cyber Auth Committee
- 2008-2010: Consultation & Strategy
- 2010-212: Procurement & Transition
- 2012: Services Operational: (SecureKey Concierge & GCKey)
- 2013 Conclusion (DM membership incorporated in DM SFI)

Federating Identity

- 2010: GC Guideline on Defining Authentication Working Group
- 2011: GC Guideline on Identity Assurance Working Group
- 2013: GC Pilot Projects (Individuals/Businesses)
- 2013: GC Policy & Legal Implications Working Group
- 2014 Canada's Digital Interchange
- 2015 Identity Linkages Project

Task Force for Payments System Review

- 2012: Recommendation to create Digital Identification and Authentication Task Force (DIAC)
- 2015: DIACC Trust Framework Working Group

Identity Management Sub-Committee (IMSC)

- 2012: Changed Reporting Structure to Joint Councils
- 2013: IMSC Working Group

International

- 2013-2015: Identity Summits
- Involvement in Kantara, ISO & ANSI Standards

DM Committee on Service and Federating Identity (SFI)

- 2013: Inaugural meeting

Related Arrangements & MOUs

- Citizenship Certificate Validation (CIC & Provinces)